HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80528-9599

08-21-00

PATENT APPLICATION

ATTORNEY DOCKET NO. 10001687-1

08/17/00 2004 U.S. PTO

IN THE U.S. PATENT AND TRADEMARK OFFICE
Patent Application Transmittal Letter

08/17/00 jc864 U.S. PTO 09/641929

ASSISTANT COMMISSIONER FOR PATENTS
Washington, D.C. 20231

Sir:

Transmitted herewith for filing under 37 CFR 1.53(b) is a(n): (X) Utility ( ) Design
(X) original patent application,
( ) continuation-in-part application

INVENTOR(S): **Kevin G. Currans**

TITLE: **Assured Printing Of Documents Of Value**

Enclosed are:

(X) The Declaration and Power of Attorney. (X) signed ( ) unsigned or partially signed

(X) 14 sheets of drawings (one set) ( ) Associate Power of Attorney

( ) Form PTO-1449 (X) Information Disclosure Statement and Form PTO-1449

( ) Priority document(s) ( )(Other) _____ (fee $_____)

CLAIMS AS FILED BY OTHER THAN A SMALL ENTITY				
(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) TOTALS
TOTAL CLAIMS	23 — 20	3	X $18	$ 54
INDEPENDENT CLAIMS	7 — 3	4	X $78	$ 312
ANY MULTIPLE DEPENDENT CLAIMS	0		$260	$ 0
BASIC FEE: Design $310.00); Utility $690.00)				$ 690
TOTAL FILING FEE				$ 1,056
OTHER FEES				$
TOTAL CHARGES TO DEPOSIT ACCOUNT				$ 1,056

Charge $ 1,056 to Deposit Account 08-2025. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16, 1.17,1.19, 1.20 and 1.21. A duplicate copy of this sheet is enclosed.

"Express Mail" label no. EL550209696US

Date of Deposit August 17, 2000

I hereby certify that this is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231.

By Raymond A Jenski

Typed Name: Raymond A. Jenski

Respectfully submitted,

Kevin G. Currans

By Raymond A Jenski

Raymond A Jenski
Attorney/Agent for Applicant(s)
Reg. No. 31,267
Date: August 17, 2000
Telephone No.: (541) 715-8441

Rev 12/99 (TransNew)

- Attach as First Page to Transmitted Papers -

ASSURED PRINTING OF DOCUMENTS OF VALUE

Field Of The Invention

The present invention relates generally to secure document printing. In particular, the present invention relates to a method and apparatus for establishing that a document represented by a computer file that was sent via a data network, was paid for and successfully printed from a remote printing device.

Related Applications

The present application is related to patent applications concurrently filed herewith, the respective teachings of which are incorporated by reference. These related applications are U.S. Patent Application Docket Nos. 10001062 by Currans et al., titled "Method and Apparatus For Insuring Output Print Quality" (hereinafter "Guaranteed Print"), and 10001686 by Currans, entitled "Serialized Original Print" (hereinafter "Serialized Print"). As of the filing date of this application and these related applications, all rights, title and interests are commonly owned by the Hewlett Packard Company.

Background Of The Invention

The Internet, and in particular the World Wide Web, has enabled the instantaneous transfer of electronic files between computers that might be located anywhere in the world so long as the computers are coupled to the Internet. Because these files routinely represent documents, photographs, or perhaps bank account, credit card account numbers, all of which have economic value, the speed at which intellectual property and money can be transferred is now nearly instantaneous.

While the ease and speed with which documents and value can be transferred can be a boon to business it can also be a liability when the distribution of an electronic file needs to be

controlled. By way of example, if a valuable work of art such as a photograph, is digitized (i.e. converted into an electronic file), uncontrolled reproduction and distribution of the electronic file that represents the art work will eventually render the work valueless. Electronically transferring files that have any sort of economic value is problematic because of the likelihood that economic value will be taken by those who are unscrupulous.

With the advent of electronic commerce, and the accompanying worldwide distribution of documents and other valuable information, a way of discerning that a document has been delivered to, and printed by, an intended recipient might prevent or reduce instances of fraud enabled by the ease with which electronic files can be reproduced and distributed.

Summary Of The Invention

The present invention provides a method and apparatus for controlling printing of a document delivered via a computer network. A first portion of a document is encrypted using at least a first encryption key, thereby creating a partially encrypted file. The partially encrypted file is transmitted via the computer network. A second portion of the transmitted partially encrypted file is printed and a t least a serialized print number is returned. In response, the first encryption key is received. The first portion of the partially encrypted file is then decrypted and printed.

Brief Description Of The Drawings

Figure 1 is a simplified block diagram of a computer network including a sender's computer and a document recipient's computer and printer.

Figures 2-1 through 2-13 show a data flow diagram or transaction timeline representation of the commands and signals exchanged between the various computers, software and printers that implement the claimed process.

Detailed Description Of The Preferred Embodiments

Briefly stated, the present invention provides a method and apparatus for verifying that a document was printed from an electronic file that was transmitted to and printed from a remote print mechanism. The exemplary method disclosed herein enables a document or file distributor to control re-distribution by conclusively determining whether a document printed

from a file was printed in whole or in part. In a preferred embodiment, the process includes the steps of encrypting a document and/or parts thereof that is to be transferred electronically, transmitting the encrypted document to an intended party via a data network, such as the Internet, partially decrypting the document using a first decryption key so as to enable the document to be verified that it was properly received, and printing part of the document up to a point at which a second decryption key is required.

If the document is successfully printed down to the point where a second encryption key is required, the recipient of the document returns to the sender, an indicia, such a serial number of the document, which has been physically printed on the document at the time, that the document had started to print successfully. Receipt of the partial-printing proof by the document sender triggers the transmission to the document recipient (i.e., the printer and not the user's browser), the second decryption key by which the remaining portion of the document can be decrypted and printed by the recipient (i.e., the printer and not the user's browser). Receipt of the indicia that the document was at least partially printed is created by the recipient's printer or print mechanism using a method disclosed and claimed in "Serialized Print".

Upon the document sender's receipt of the indicia that the document was at least partially printed, the document recipient will thereby have provided to the document sender, conclusive proof that the entire document was received successfully. By using the "Guaranteed Print" technology, the accuracy of the document that was printed can be determined and a numerical indicia of output print quality generated such that a document sender provided with the print quality indicia can know whether the document that was printed was in fact a reasonably facsimile of the document that was electronically sent. Using the indicia of printing that was received by the sender, as well as an objective indicia of the output print quality documents that are sent electronically but which do not reasonable resemble their original condition as sent by the sender can be selectively retransmitted by the document sender at the document sender's discretion.

Figure 1 shows a simplified block diagram of a registered printing system 100 by which computer files are electronically transferred over a network, to be printed at a remote device. The system 100 is comprised of a network, such as the Internet, which is a data network 102 comprised of a number of computers 104 intercoupled to each other via appropriate media 106

and switching systems (not shown). An explanation of computer networks is beyond the scope of this disclosure and not necessary for an appreciation of the invention disclosed herein. It is sufficient to state that electronic files are transferred between computers over the network. In addition to the Internet, other data transfer mechanisms such as Ethernet networks, local area networks, wide area networks or direct dial-up connections using one or modems (not shown) could be used to accomplish file transfers. The transferred files might represent a variety of documents, such as works of art, photographs, negotiable instruments, vouchers or other means of sending or receiving documents having economic value to either the sender or recipient. When such documents are printed, they typically have or represent economic value to the sender, the recipient, or a third party.

Document transfers between document senders and receivers are enabled by way of a network like the Internet but as set forth above, such transfers also might be accomplished using a local area network, a wide area network, an Ethernet network as well as the plain old telephone system sometimes referred to as the public switched telephone network. In instances where the data network 102 is the World Wide Web of the Internet, a web browser program executing on a subscribers computer 108 provides access to "web sites" that are embodied by other computers 104 coupled to the web, including the computer(s) of a document provider, identified in Figure 1 by reference numeral 110.

By way of example, a subscriber's computer 108 might request the computer of a content provider 110 to transfer to it, some sort of electronic file 112, embodying a document that might include a work of art, a memorandum, or perhaps a negotiable instrument or airline tickets for example. Upon being printed, such a document has economic value to either the sender (not shown) or the recipient of the document (not shown).

Using the Internet 102, an intended recipient of a document, considered herein to be a document requestor, can request from a sender's computer 110, the transmission of a file 112 from the sender's computer 110 via the Internet 102 to the recipient's computer 108. If the recipient's computer 108 has the requisite application program by which the transmitted file 112 can be opened and printed, printing the document 114 that was embodied as an electronic file 112 is readily accomplished using an appropriate printer 116 coupled to the recipient's computer 108.

In the preferred embodiment of this invention, the recipient's computer 108 and the printer 116 are equipped with, and capable of using, the method and apparatus disclosed in "Serialized Print." As such, the printer 116 is a printer that is capable of generating serialized output as described in "Serialized Print". The disclosure and teachings of the "Serialized Print," by which the generation of serialized output is taught, is incorporated herein by reference. Using that novel method for generating serialized printed output, the printer 116 generates a unique serial number, bar code or encoded data (hereafter, serial number) for the document 114 in the course of printing the file 112. The serial number generated by the printer 116 is of paramount importance in verifying to a document sender that the file 112 was received at the computer 108 and at least partially printed.

Figures 2-1 through 2-13 shows a data flow diagram depicting the steps of the method described herein.

In Figure 2-1, as an initial matter, the software capability to guarantee output print quality and to produce a serialized original print needs to be installed on the recipient's computer 108 as well as on the sender's computer 110 as depicted in step no. 202. Assuming that such software capabilities have been installed on the respective first and second computers, the recipient's (i.e. second) computer 108 will request from the printer 116 an encryption key for public distribution (i.e. a public encryption key) in the format of an X.509 certificate, which might be embodied as a serial number, a model number or combination thereof obtained from the printer in step no. 204 in Figure 2-1.

In Figure 2-2, when the printer returns an X.509 certificate and data as that identifies the capabilities of the printer (For example, is the printer capable of practicing the "Guaranteed Print " technology) at step 206, the user's computer installs the public key on a browser plug-in file, known to those skilled in the art.

Information about the X.509 standard is available from a variety of sources, including the National Institute of Standards and Technology web site, the URL of which is: http://csrc.ncsl.nist.gov/. An X.509 certificate serves as an electronic credential over the Internet for individuals and computer services (Web sites). X.509 certificates are used in the same way as birth certificates, passports or drivers' licenses to validate the identity of individuals for Web site access, communication and electronic commerce.

An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet.

The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply. The most widely used standard for digital certificates is X.509 which is the technology used by this merchant.

The X.509 is currently believed to be the most widely used standard for defining digital certificates. The X.509 standard for digital certificates binds the identity of a person or organization to an electronic identification key. The digital certificate contains information about its owner, its issuer, issue and expiration date stamps, and information for verifying the integrity of the certificate that can be used for digital IDs, digital signatures and electronic fingerprints.

By executing an HTTP (hypertext transfer protocol) "GET" command, the user's web browser (e.g. Internet Explorer™ or Netscape™) running on the user's computer (i.e. the second computer) requests verification of the printer's public key from a security key issuer, which then posts the answer of authenticity of the printer's public key using a "PUT" in step 207. In Figure 2-3, in step 208, a "certificate" from a printer capable of practicing the "Guaranteed Print" technology is decrypted and the printer's public key is installed (or copied) into the document purchaser's web browser. A decision to buy a document is formatted and sent to the vendor 210 conveying the capabilities of the printer, i.e. that the printer is "Guaranteed Print" technology capable.

In Figure 2-4, the document vendor's computer's response 212 is to transmit a file (identified in Figure 1 by reference numeral 112) at least part of which is encrypted at least once using a so called public key of the vendor's computer (identified in Figure 1 by reference numeral 110) and preferably also encrypted using a uniform resource locator (URL) address to which credit or payment information is to be sent by the buyer.

In an alternate embodiment, only part of a document is encrypted prior to transmission and using only one key. By encrypting only part of a document (i.e. up to a predetermined point) prior to transmission, at least the unencrypted portion of the document can be printed at the destination, without a decryption key, thereby establishing recognition-of-value by the purchaser before transferring funds. In such an embodiment, a decryption key eventually needs to be provided. By holding back the decryption key pending receipt of payment – and perhaps ascertaining proof that at least part of the document was satisfactorily printed using for example the "Guaranteed Print" teachings - a document vendor can protect its interest in the document by withholding the key until payment has been received by an entity associated with the document, for example, the vendor or a credit agency for the vender.

In step 214, the document buyer's computer (i.e. the second computer 108) optionally retrieves the URL of a credit agency and performs a secure hypertext transfer protocol transfer providing payment information to a financial organization or other credit provider effectuating the transfer of funds for the payment of the file from the vendor. A credit approval transfer form 216 is optionally returned to the buyer and enables the buyer to populate the form with pertinent credit information by which the credit provider can make payment to the vendor in step 218, shown in Figure 2-5. If the credit transaction is validated by the credit provider as set forth in step 220, the transaction can be memorialized by the buyer's computer and thereafter forwarded to the vendor in step 222, shown in Figure 2-6.

The document vendor can electronically verify with a credit provider, e.g. www.cybercash.com, in step 224 that the document purchaser has funded, or can otherwise pay for the transaction and, in response thereto, the credit provider can provide an appropriate acknowledgement 226 to the vendor, as shown in Figure 2-7. Upon verification that payment will be received by the document vendor, the vendor optionally encrypts the information content of interest, using the document vendor's private key and a second key (also known as a session key) and sends the doubly encrypted file to the purchaser in step 228. (Public key/ private key encryption and decryption mechanisms are well known. Disclosure or understanding of that technology is not germane to the invention disclosed herein. Alternate embodiments of the invention include singly encrypting the file using a single encryption key, which as an example could be the document vendor's private key, a purchaser's public key or

some other encryption key by which the document could be secured against theft in transit across a data network or by the document recipient.)

In Figure 2-8, using his own private decryption key, the purchaser decrypts the file and verifies that the received file is intact and sends the file to the printer 116 for printing in step 230. The printer begins printing the file and in the process generates an original serialized print number in accordance with the "Serialized Print" methodology, in step 232. The serial number generated by the printer will be printed and also sent to the browser of the purchaser's computer in step 234, shown in Figure 2-9. The browser also records the serial number of the print job in progress for subsequent use.

As the printer 116 continues following the instructions from the computer 108 to generate output, eventually the printer 116 or the computer 108 encounters information in the file 112 that is encrypted with the vendor's second key. Upon determining that further printing will be inhibited absent the other decryption key, the printer, using the "Serialized Print" methodology, requests the second key in step 236 from the user's computer, Figure 2-9. In step 238, Figure 2-10 the user's browser transmits a request for the second key to the printer or in this case the vendor's computer 110 and as proof that the job has been at least partially printed includes the serialized print number generated by the printer in step 232.

Upon receipt of the original serial print number generated in step 232 by the vendor's computer 110 in step 238, the vendor can assume that at least part of the document file 112 was printed from the printer 116 and was fully and successfully received by the computer 108. The vendor can record the serialized print number in a database for billing purposes or for billing credit purposes.

The vendor can also optionally submit the transaction complete signal in step 240, Figure 211, to the credit provider as a means for justifying the receipt of payment from the credit provider. Upon receipt that at least part of the document has been printed, the credit provider can debit the purchasers account and credit the vendor's account accordingly.

In order to complete the printing job, the vendor's computer 110 needs to return to the purchaser's computer 108, the second decryption key in step 242 or a session key, that the printer can use for decrypting the content The second key is encrypted so only the printer can decrypt it. This is generally done using the printer's public key and the vendor's private key. Upon receipt of the second key, the browser running on the purchaser's computer 108 passes

the second encryption key to the printer in step 244, which enables the printer to decrypt the key and finish the print job it started in step 230 by decrypting the document and printing it. In step 246, the printer sends status information back to the browser of the purchaser's computer 108 informing the purchaser's computer 108 and possibly the browser of whether or not the entire print job was successful.

By using the methodology disclosed in the inventor's "Guaranteed Print" technology, the printer 116 can provide an objective measurement of the output print quality. A printer employing the "Guaranteed Print" technology is referred to herein as a printer that is capable of guaranteeing output print quality.

Using the "Guaranteed Print" technology, the printer 116 depicted in Figure 1 can, in real time, compare what was printed to what was sent 112 and determine whether or not the purchaser got what he or she bargained for. Using that technology it is possible to create a numeric index of the relative output quality of a print job from a printer.

If output print quality was determined to be unsatisfactory or failed altogether, the printer 116 can send an appropriate error message to the vendor or the vendor's computer 110 informing the vendor that the output print quality was defective. In the event that an output print job did not successfully complete in its entirety, or was otherwise disturbed or defective, the vendor can impede retransmission of the file 112 until it physically receives all of the output that was printed by the printer 116.

By way of data recovered using the method and apparatus for insuring output print quality, the vendor knows precisely how much of the document file 112 was actually printed 114 and refuse to provide another copy of the document until physical receipt of the output print material is received in hand that has the serial number, bar code or encoded data in step 234.

Public and private encryption key technologies are well known to those skilled in the art. Alternative embodiments of the invention would include using proprietary keys of both the purchaser and the vendor. By using a publicly available key however, it is possible for the document sender to encrypt a file with a public key enables the document recipient to decrypt it using his private key. Commercially available public/private encryption software is readily available.

It should be apparent that by using the methodologies disclosed herein, that valuable documents can be transferred via data networks with some sense of security and with some sense that unauthorized reproduction of a document will be impeded. Similarly, valuable content for which value was received need not be retransmitted absent proof by the sender that the intended output was not successfully realized.

We claim:

CLAIMS

1. A method to control printing of a document file delivered via a computer network comprising the steps of:

at a first computer:

encrypting at least a first portion of a document file using at least a first encryption key thereby creating a partially encrypted file;

transmitting the partially encrypted file to a second computer via said computer network;

at said second computer:

printing at least a second portion of said partially encrypted file using a serialized print methodology;

returning to said first computer at least a serialized print number, and receiving, in response thereto, said first encryption key;

decrypting said first portion of said partially encrypted file to create a decrypted document file; and

printing said decrypted document file.

2. A method in accordance with the method of claim 1 wherein said step of returning further comprises the step of providing payment.

3. A method in accordance with the method of claim 1 further including steps of:

before transmitting the partially encrypted file to a second computer, encrypting at least part of said partially encrypted file to form a twice-encrypted file using a second encryption key; and

prior to printing at least a second portion of said partially decrypted file, decrypting said twice-encrypted file using at least one of either said second encryption key or a third encryption key.

4. A method in accordance with the method of claim 1 wherein said serialized print methodology includes the steps of:

generating by a device printing said decrypted document file, a number correlating said decrypted document file to said printing device;

returning said number to said first computer thereby enabling said second computer to receive said first key.

5. A method in accordance with the method of claim 1 further including the step of printing at least a portion of said partially decrypted document file using a guaranteed print methodology.

6. A system for controlling the printing of a document file delivered via a computer network comprising:

a first computer that encrypts at least a first portion of a document file using a first key;

a data transfer device coupled said first computer capable of transferring the partially encrypted document file to a second computer;

a print mechanism operatively coupled to said data transfer device, said print mechanism capable of receiving said document file and decrypting at least a portion of said first portion of said document file and printing said first portion using a serialized print methodology.

7. The system of claim 6 wherein said print mechanism is comprised of a computer operatively coupled to a printer.

8. The system of claim 6 wherein said print mechanism is comprised of a printer capable of generating serialized output.

9. The system of claim 6 wherein said print mechanism is comprised of a printer capable of guaranteeing output print quality.

10. Apparatus for controlling the printing of a document file delivered via a computer network, comprising:

a first computer coupled to a data transfer mechanism, said first computer capable of receiving via said data transfer mechanism, at least one partially encrypted document file from a second computer;

a print mechanism operatively coupled to said first computer, said print mechanism being capable printing at least a portion of said partially encrypted document file using a serialized print methodology.

11. Apparatus for controlling the printing of a document file delivered via a computer network comprising:

a first computer coupled to a data transfer mechanism, said first computer capable of receiving via said data transfer mechanism, at least one partially encrypted document file from a second computer; and

a print mechanism operatively coupled to said first computer, said print mechanism being capable printing at least a portion of said partially encrypted document file using a guaranteed print methodology.

12. A method of controlling the printing of a document delivered via a computer network comprising the steps of:

printing a first portion of the document, said first portion being unencrypted;

communicating, via the computer network, with an entity associated with the document to arrange for the printing of a remaining portion of the document

receiving, as a result of said communicating step, an encrypted remaining portion of the document;

decrypting said remaining portion; and

printing said decrypted remaining portion.

13. A method in accordance with the method of claim 12 wherein said communicating step further comprises the step of providing payment to said entity.

14. A method in accordance with the method of claim 12 wherein said communicating step further comprises the step of ascertaining quality of said printed first portion.

15. A method in accordance with the method of claim 12 further comprises the step of generating a number correlating said document to a printing device printing said first portion.

16. A method in accordance with the method of claim 15 wherein said step of communicating further comprises the step of communicating said generated number.

17. A method of controlling the printing of a document delivered via a computer network to a user, comprising of the steps of:

encrypting a portion of the document;

transmitting an unencrypted portion of the document via the computer network to the user for printing;

receiving a communication related to a reception of said unencrypted portion by the user; and

transmitting said encrypted portion of the document to the user via the computer network in response to said receiving step.

18. A method in accordance with the method of claim 17 wherein said receiving step further comprises the step of receiving a payment for the document.

19. A method in accordance with the method of claim 17 wherein said receiving step further comprises the step of receiving a proof that said unencrypted portion of the document was satisfactorily printed

20. A method of controlling the printing of a partially encrypted document file delivered via a computer network, at least a first portion of which partially encrypted document is encrypted using at least a first encryption key, comprising the steps of:

printing at least a second portion of the partially encrypted document file;

creating a serialized print number and returning the serialized print number via the computer network;

receiving the first encryption key;

decrypting the first portion to create a decrypted document file; and

printing said decrypted document file

21. A method in accordance with the method of claim 20 further comprising the step of providing payment for the partially encrypted document.

22. A method in accordance with the method of claim 20 wherein at least part of the partially encrypted document file is further encrypted to form a twice-encrypted file using a second encryption key, further comprising the step of prior to printing at least a second portion of said partially decrypted document file, decrypting said twice-encrypted file using at least said second encryption key.

23. A method in accordance with the method of claim 21 wherein said step of creating a serialized print number further comprises the step of generating, by a device printing said decrypted document file, a number correlating said decrypted document file to said printing device.

ASSURED PRINTING OF DOCUMENTS OF VALUE

ABSTRACT OF THE DISCLOSURE

The transmission and reproduction of an original document transferred via a data network can be assured when the printing mechanism generates a unique serial number for the document being printed. The sender of the document is assured that the intended recipient received the document, paid for it, and was able to print it by receipt of the unique serial number and a request for an encryption key by which certain information in the document was encrypted.

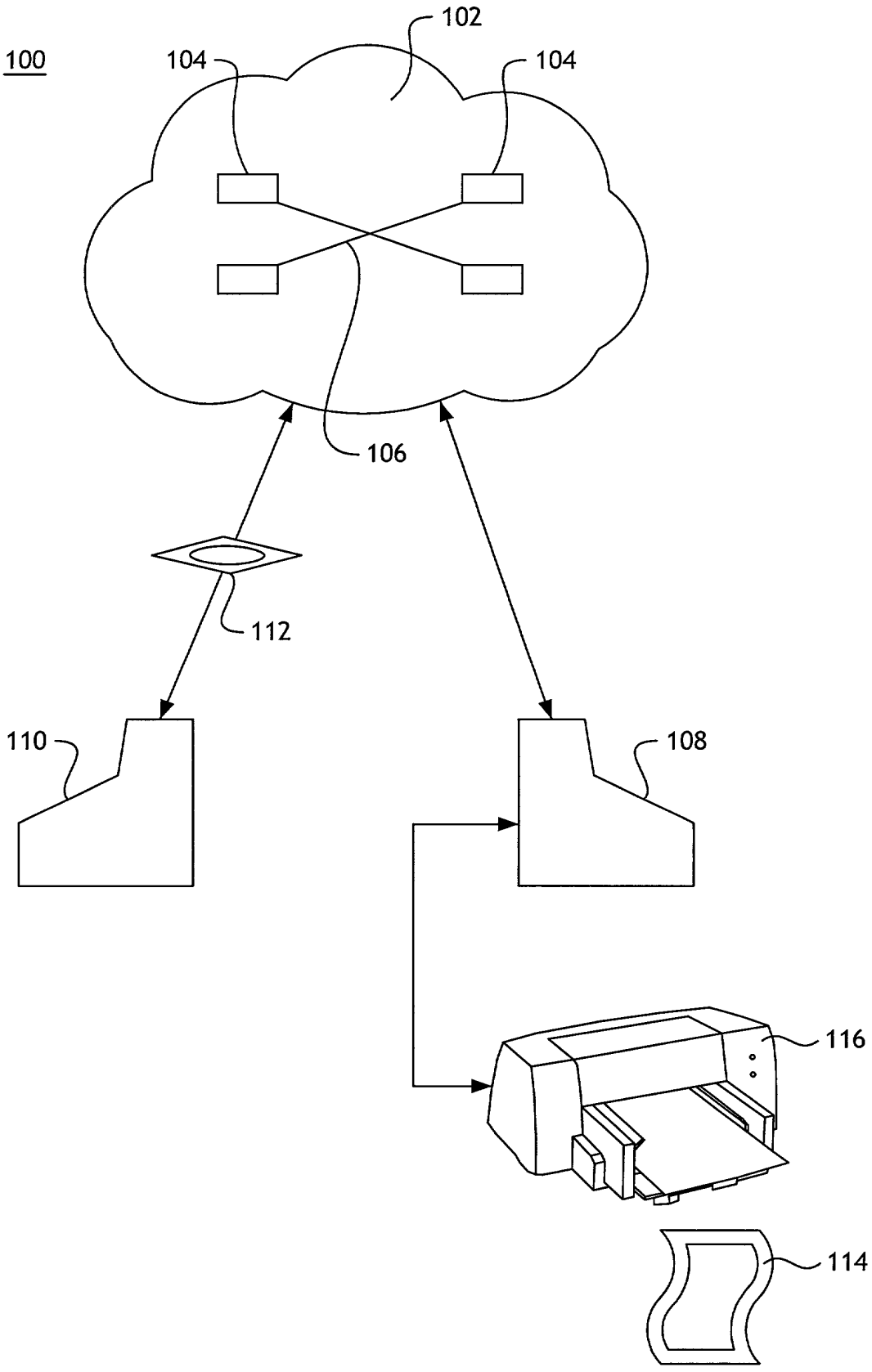

Fig. 1

"REGISTERED PRINT" PRINTER	
COMMUNICATIONS BETWEEN PRINTER AND BROWSER	204 ~ REQUEST PRINTER NAME, PUBLIC KEY, "REGISTERED PRINT" ABILITIES
"USER BUY PRODUCT" CLIENT - BROWSER	INSTALL "REGISTERED PRINT" ON SYSTEM W/ SUPPORTING PRINTER (ONE THAT HAS GUARANTEED PRINT AND ORIGINAL PRINT) ~ 202
NETWORK TRAFFIC BETWEEN CLIENT AND VENDOR	
VENDOR	
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND CLIENT	
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND VENDOR	
CREDIT HOLDER	
CA - CERTIFICATE AUTHORITY (E.G. GTE, VERISIGN)	

Fig. 2-1

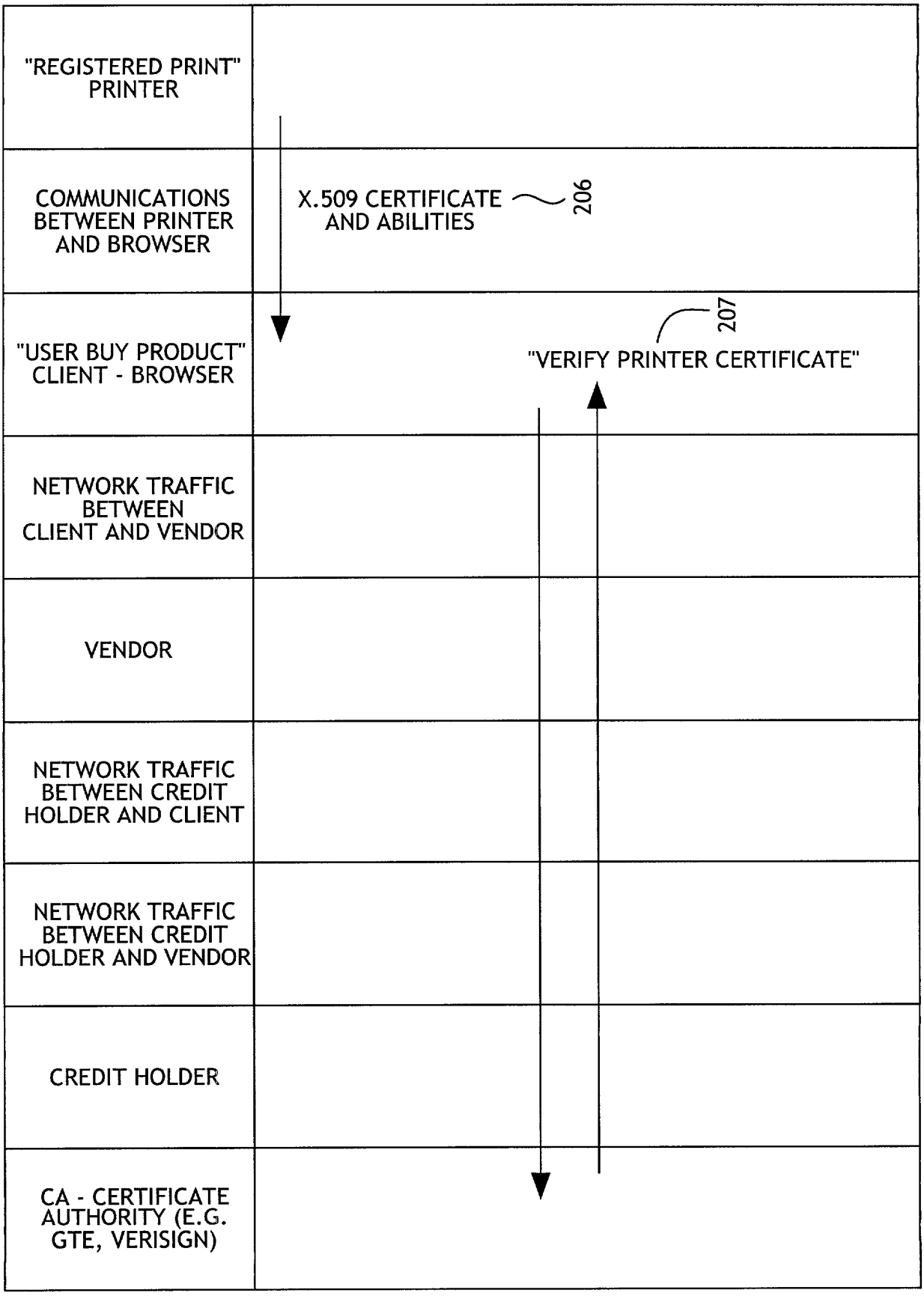
"REGISTERED PRINT" PRINTER
COMMUNICATIONS BETWEEN PRINTER AND BROWSER
X.509 CERTIFICATE AND ABILITIES
206
"USER BUY PRODUCT" CLIENT - BROWSER
207
"VERIFY PRINTER CERTIFICATE"
NETWORK TRAFFIC BETWEEN CLIENT AND VENDOR
VENDOR
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND CLIENT
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND VENDOR
CREDIT HOLDER
CA - CERTIFICATE AUTHORITY (E.G. GTE, VERISIGN)

Fig. 2-2

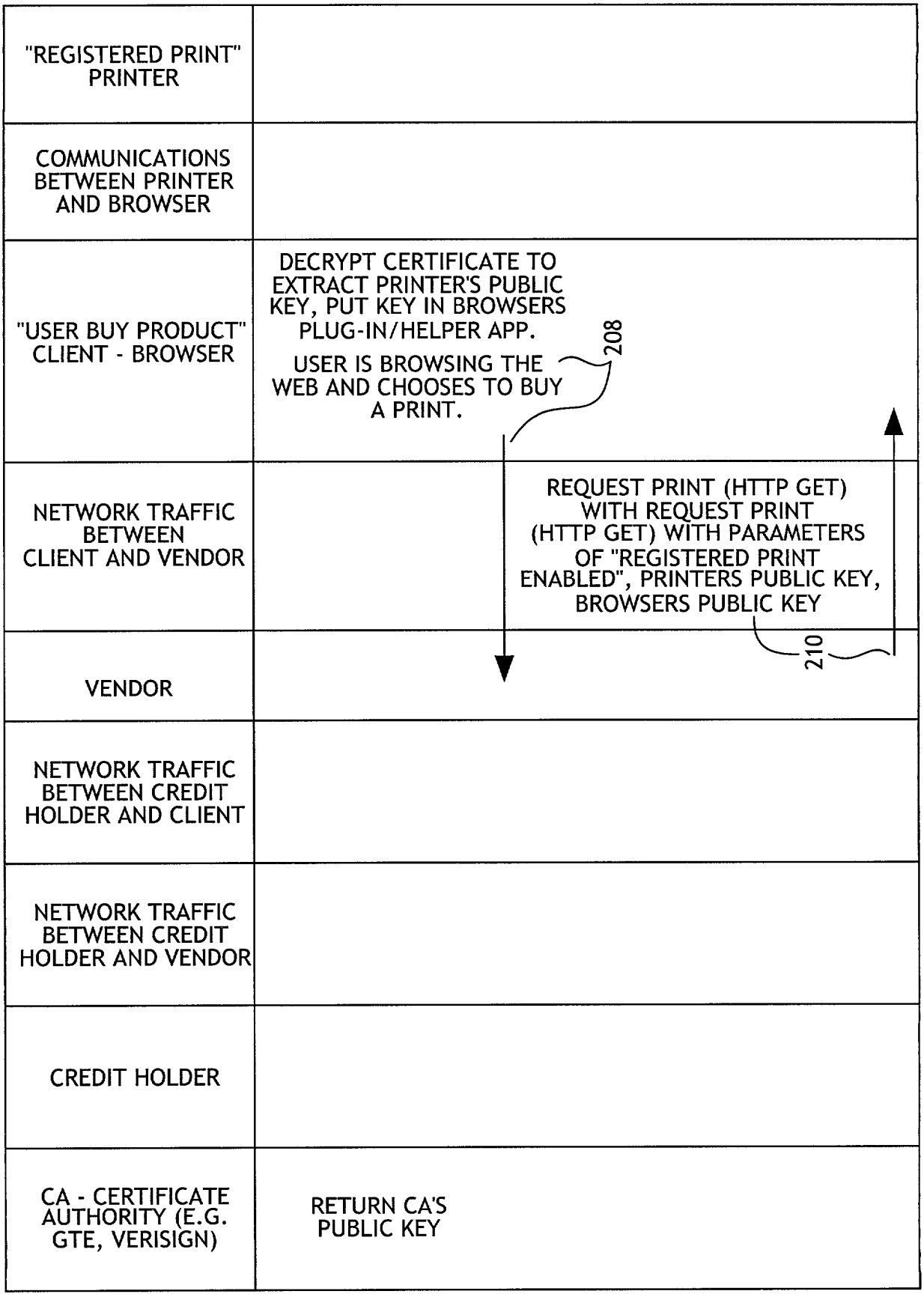
"REGISTERED PRINT" PRINTER
COMMUNICATIONS BETWEEN PRINTER AND BROWSER
"USER BUY PRODUCT" CLIENT - BROWSER
NETWORK TRAFFIC BETWEEN CLIENT AND VENDOR
VENDOR
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND CLIENT
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND VENDOR
CREDIT HOLDER
CA - CERTIFICATE AUTHORITY (E.G. GTE, VERISIGN)
DECRYPT CERTIFICATE TO EXTRACT PRINTER'S PUBLIC KEY, PUT KEY IN BROWSERS PLUG-IN/HELPER APP.
USER IS BROWSING THE WEB AND CHOOSES TO BUY A PRINT.
208
REQUEST PRINT (HTTP GET) WITH REQUEST PRINT (HTTP GET) WITH PARAMETERS OF "REGISTERED PRINT ENABLED", PRINTERS PUBLIC KEY, BROWSERS PUBLIC KEY
210
RETURN CA'S PUBLIC KEY

Fig. 2-3

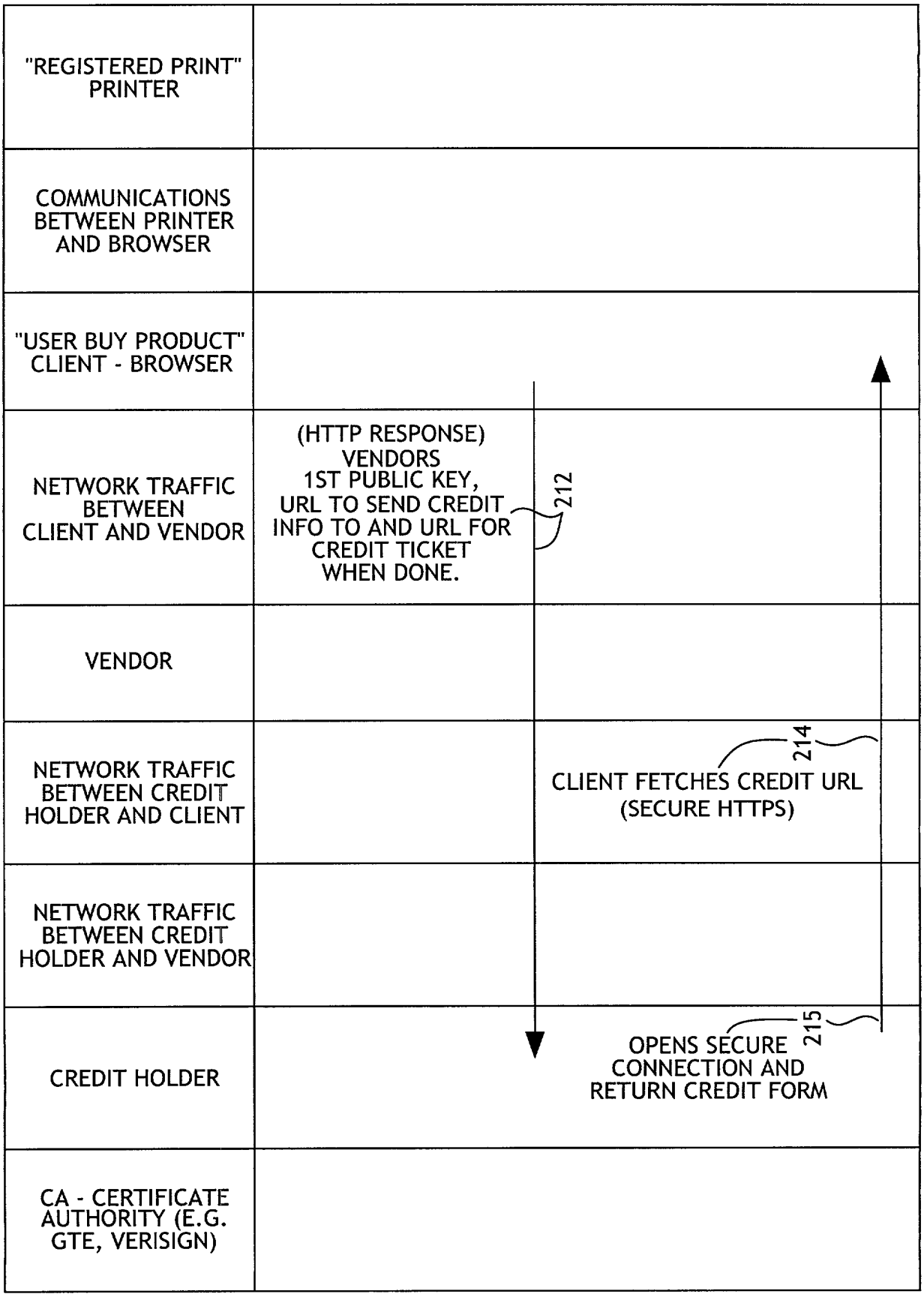
"REGISTERED PRINT" PRINTER
COMMUNICATIONS BETWEEN PRINTER AND BROWSER
"USER BUY PRODUCT" CLIENT - BROWSER
NETWORK TRAFFIC BETWEEN CLIENT AND VENDOR
(HTTP RESPONSE) VENDORS 1ST PUBLIC KEY, URL TO SEND CREDIT INFO TO AND URL FOR CREDIT TICKET WHEN DONE.
212
VENDOR
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND CLIENT
214
CLIENT FETCHES CREDIT URL (SECURE HTTPS)
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND VENDOR
CREDIT HOLDER
215
OPENS SECURE CONNECTION AND RETURN CREDIT FORM
CA - CERTIFICATE AUTHORITY (E.G. GTE, VERISIGN)

Fig. 2-4

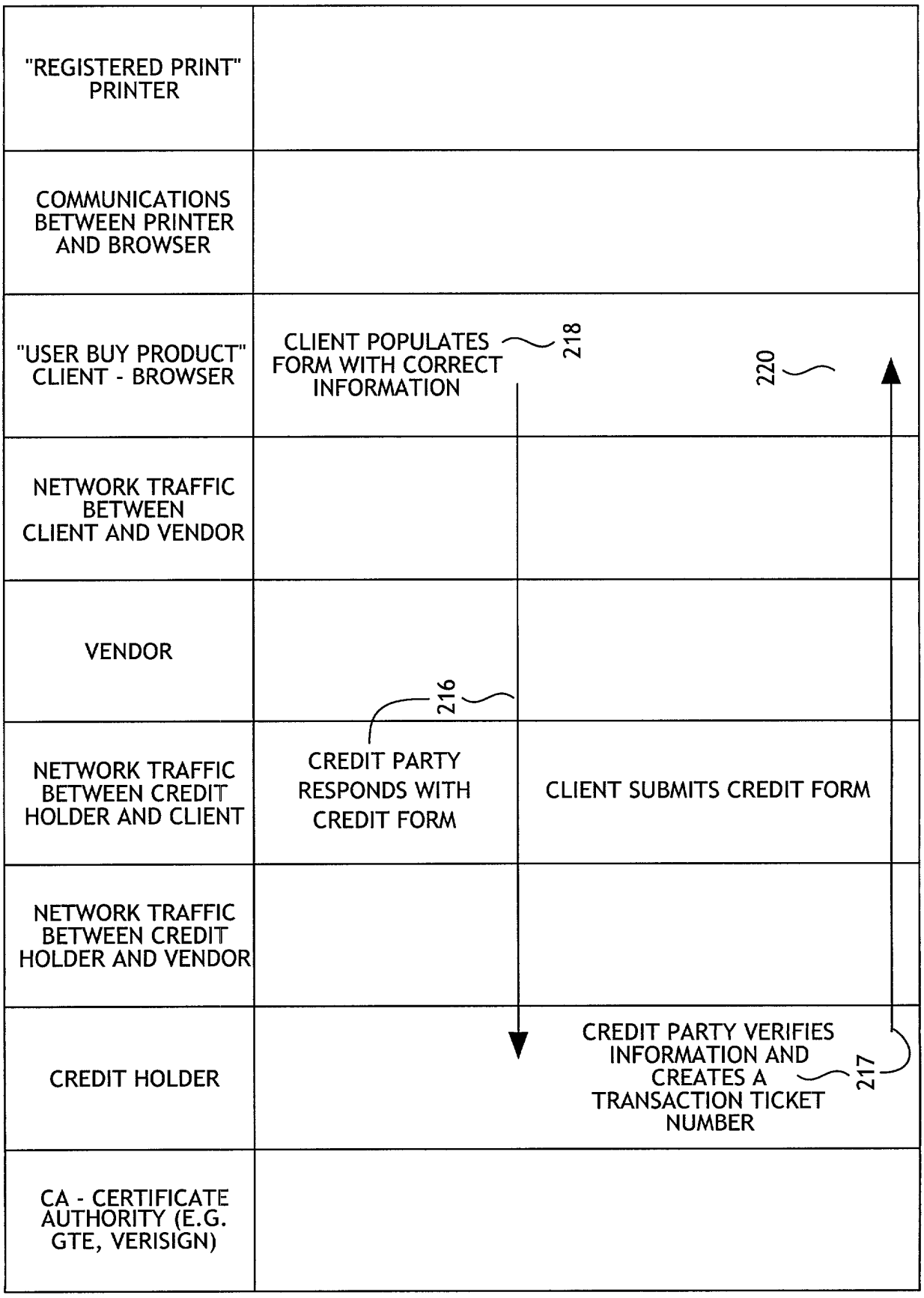
"REGISTERED PRINT" PRINTER
COMMUNICATIONS BETWEEN PRINTER AND BROWSER
"USER BUY PRODUCT" CLIENT - BROWSER
NETWORK TRAFFIC BETWEEN CLIENT AND VENDOR
VENDOR
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND CLIENT
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND VENDOR
CREDIT HOLDER
CA - CERTIFICATE AUTHORITY (E.G. GTE, VERISIGN)
CLIENT POPULATES FORM WITH CORRECT INFORMATION
218
220
216
CREDIT PARTY RESPONDS WITH CREDIT FORM
CLIENT SUBMITS CREDIT FORM
CREDIT PARTY VERIFIES INFORMATION AND CREATES A TRANSACTION TICKET NUMBER
217

Fig. 2-5

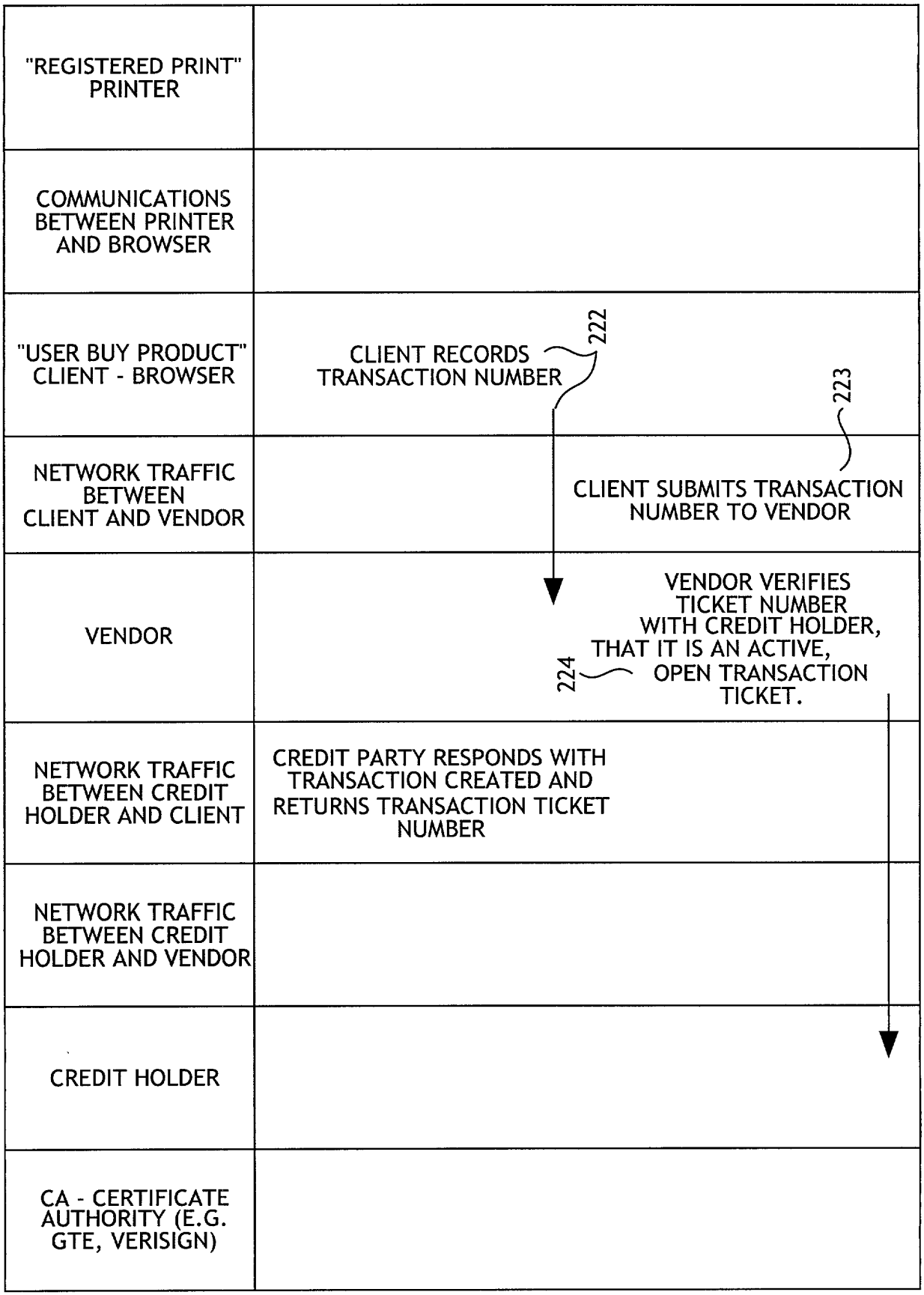
"REGISTERED PRINT" PRINTER
COMMUNICATIONS BETWEEN PRINTER AND BROWSER
"USER BUY PRODUCT" CLIENT - BROWSER
CLIENT RECORDS TRANSACTION NUMBER
222
223
NETWORK TRAFFIC BETWEEN CLIENT AND VENDOR
CLIENT SUBMITS TRANSACTION NUMBER TO VENDOR
VENDOR
VENDOR VERIFIES TICKET NUMBER WITH CREDIT HOLDER, THAT IT IS AN ACTIVE, OPEN TRANSACTION TICKET.
224
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND CLIENT
CREDIT PARTY RESPONDS WITH TRANSACTION CREATED AND RETURNS TRANSACTION TICKET NUMBER
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND VENDOR
CREDIT HOLDER
CA - CERTIFICATE AUTHORITY (E.G. GTE, VERISIGN)

Fig. 2-6

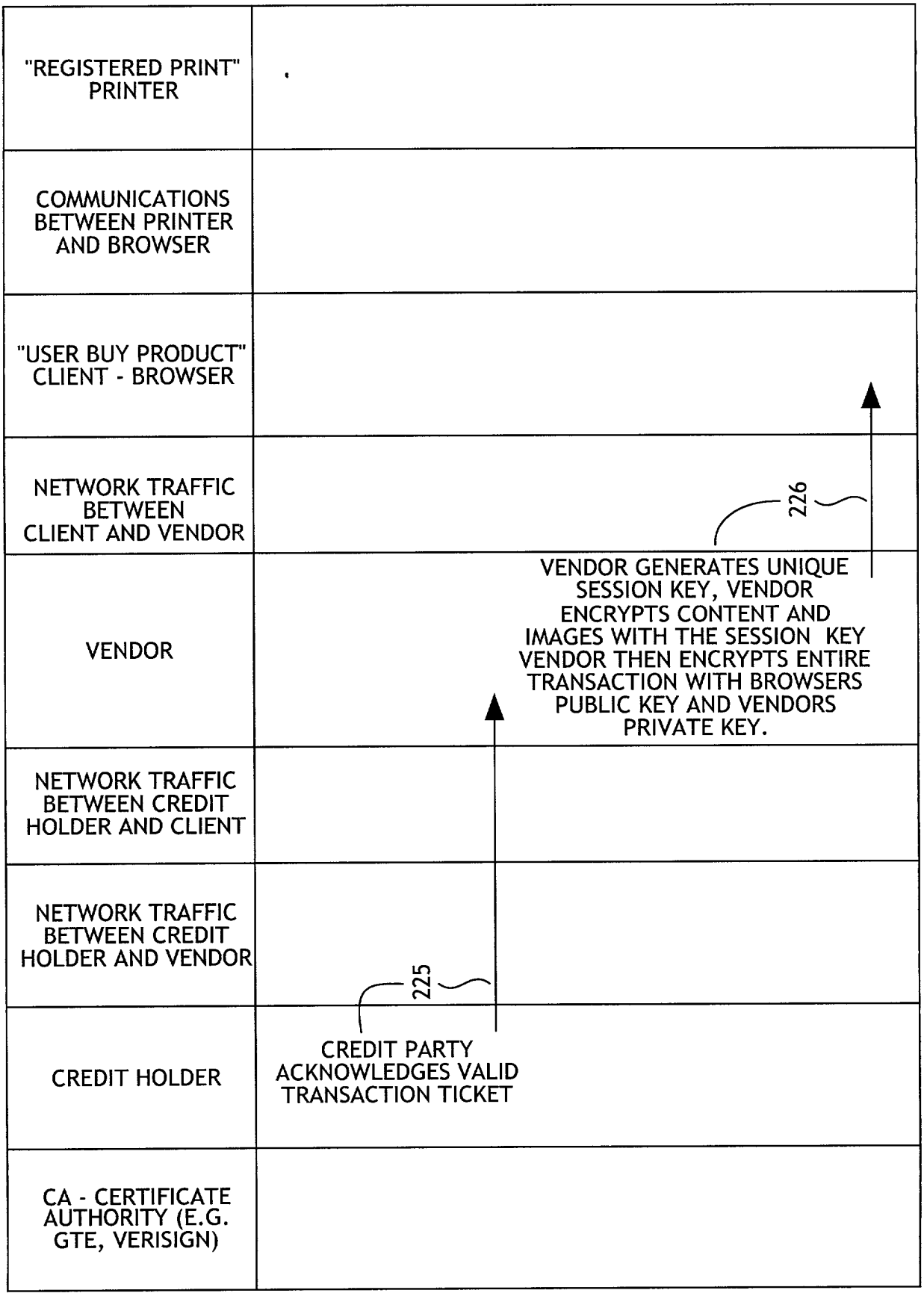
"REGISTERED PRINT" PRINTER
COMMUNICATIONS BETWEEN PRINTER AND BROWSER
"USER BUY PRODUCT" CLIENT - BROWSER
NETWORK TRAFFIC BETWEEN CLIENT AND VENDOR
226
VENDOR
VENDOR GENERATES UNIQUE SESSION KEY, VENDOR ENCRYPTS CONTENT AND IMAGES WITH THE SESSION KEY VENDOR THEN ENCRYPTS ENTIRE TRANSACTION WITH BROWSERS PUBLIC KEY AND VENDORS PRIVATE KEY.
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND CLIENT
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND VENDOR
225
CREDIT HOLDER
CREDIT PARTY ACKNOWLEDGES VALID TRANSACTION TICKET
CA - CERTIFICATE AUTHORITY (E.G. GTE, VERISIGN)

Fig. 2-7

"REGISTERED PRINT" PRINTER	PRINTER STARTS PRINTING PROCESS: GENERATES AN "ORIGINAL SERIALIZED" PRINT NUMBER, AND PRINTS IT ON THE MEDIA. 232
COMMUNICATIONS BETWEEN PRINTER AND BROWSER	230 CLIENT SEND BEGINNING OF PRINT JOB TO PRINTER
"USER BUY PRODUCT" CLIENT - BROWSER	CLIENT DECRYPTS ENTIRE JOB WITH BROWSERS PRIVATE KEY AND VENDORS PUBLIC KEY, VERIFIES IT IS ALL IN TACT, AND SUBMITS IT TO PRINTER
NETWORK TRAFFIC BETWEEN CLIENT AND VENDOR	VENDOR RESPONDS TO CLIENT WITH THE ENTIRE ENCRYPTED JOB
VENDOR	
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND CLIENT	
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND VENDOR	
CREDIT HOLDER	
CA - CERTIFICATE AUTHORITY (E.G. GTE, VERISIGN)	

Fig. 2-8

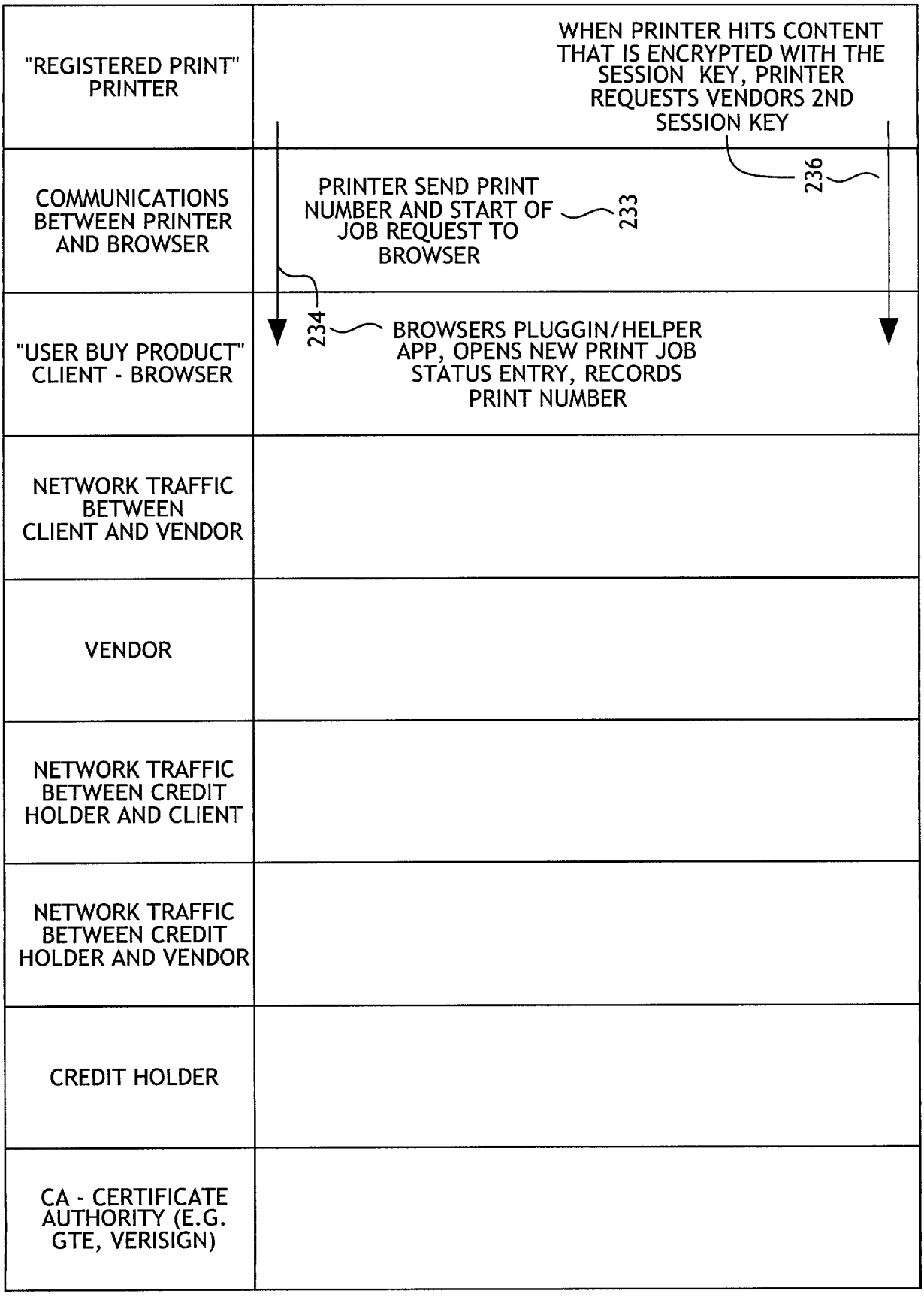
"REGISTERED PRINT" PRINTER
WHEN PRINTER HITS CONTENT THAT IS ENCRYPTED WITH THE SESSION KEY, PRINTER REQUESTS VENDORS 2ND SESSION KEY
236
COMMUNICATIONS BETWEEN PRINTER AND BROWSER
PRINTER SEND PRINT NUMBER AND START OF JOB REQUEST TO BROWSER
233
"USER BUY PRODUCT" CLIENT - BROWSER
234
BROWSERS PLUGGIN/HELPER APP, OPENS NEW PRINT JOB STATUS ENTRY, RECORDS PRINT NUMBER
NETWORK TRAFFIC BETWEEN CLIENT AND VENDOR
VENDOR
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND CLIENT
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND VENDOR
CREDIT HOLDER
CA - CERTIFICATE AUTHORITY (E.G. GTE, VERISIGN)

Fig. 2-9

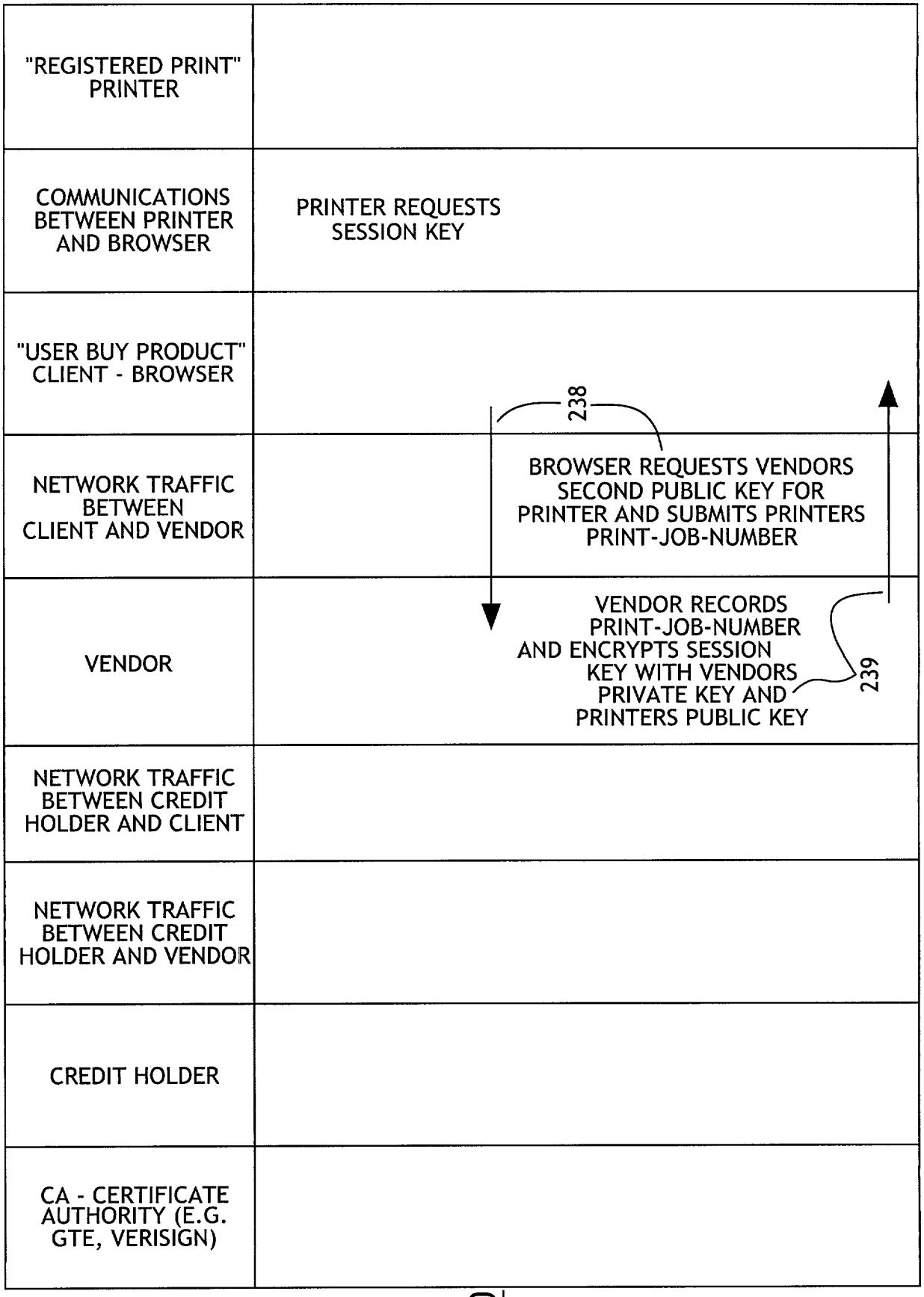
"REGISTERED PRINT" PRINTER
COMMUNICATIONS BETWEEN PRINTER AND BROWSER
PRINTER REQUESTS SESSION KEY
"USER BUY PRODUCT" CLIENT - BROWSER
238
NETWORK TRAFFIC BETWEEN CLIENT AND VENDOR
BROWSER REQUESTS VENDORS SECOND PUBLIC KEY FOR PRINTER AND SUBMITS PRINTERS PRINT-JOB-NUMBER
VENDOR
VENDOR RECORDS PRINT-JOB-NUMBER AND ENCRYPTS SESSION KEY WITH VENDORS PRIVATE KEY AND PRINTERS PUBLIC KEY
239
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND CLIENT
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND VENDOR
CREDIT HOLDER
CA - CERTIFICATE AUTHORITY (E.G. GTE, VERISIGN)

Fig. 2-10

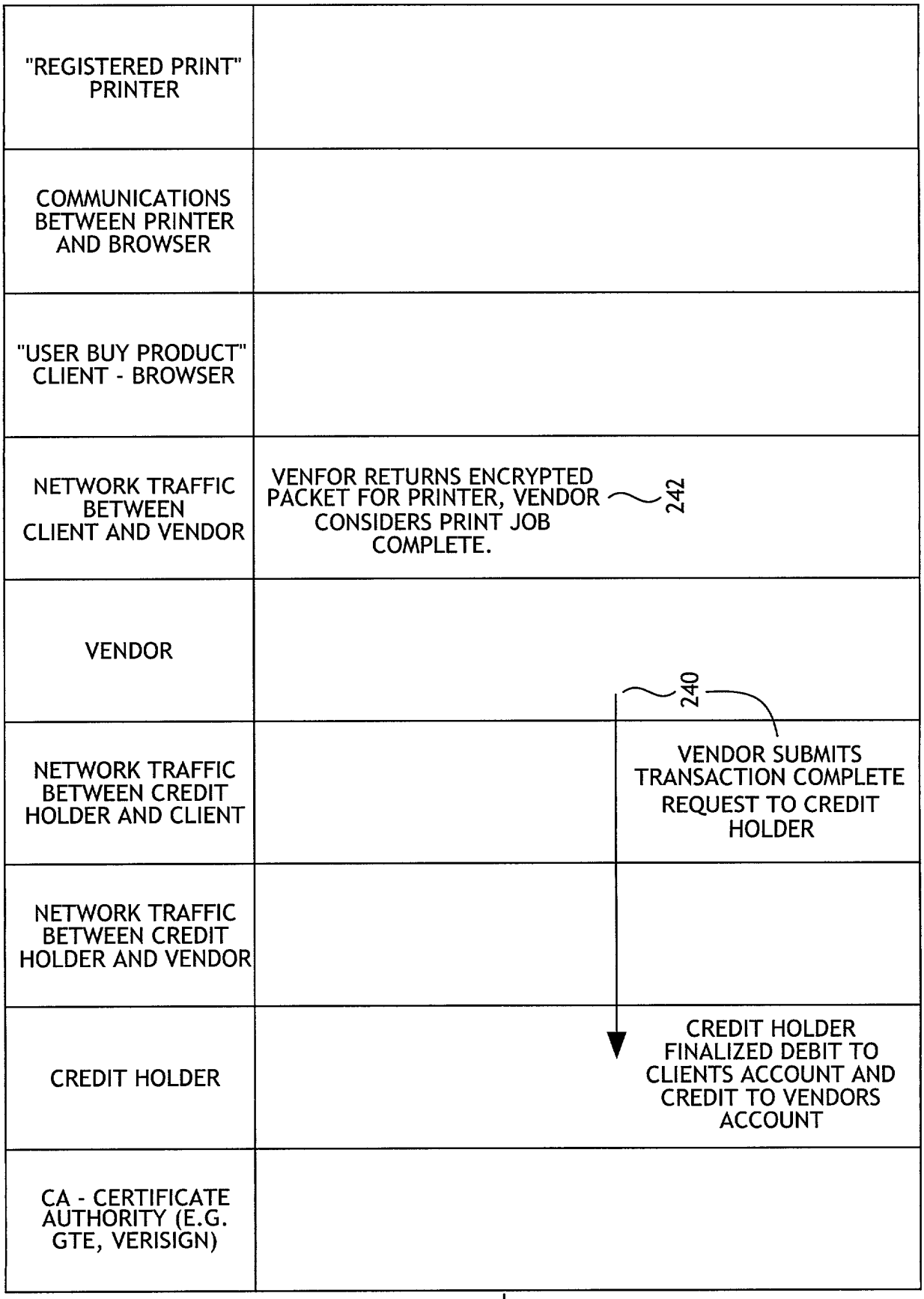
"REGISTERED PRINT" PRINTER
COMMUNICATIONS BETWEEN PRINTER AND BROWSER
"USER BUY PRODUCT" CLIENT - BROWSER
NETWORK TRAFFIC BETWEEN CLIENT AND VENDOR
VENFOR RETURNS ENCRYPTED PACKET FOR PRINTER, VENDOR CONSIDERS PRINT JOB COMPLETE.
242
VENDOR
240
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND CLIENT
VENDOR SUBMITS TRANSACTION COMPLETE REQUEST TO CREDIT HOLDER
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND VENDOR
CREDIT HOLDER
CREDIT HOLDER FINALIZED DEBIT TO CLIENTS ACCOUNT AND CREDIT TO VENDORS ACCOUNT
CA - CERTIFICATE AUTHORITY (E.G. GTE, VERISIGN)

Fig. 2-11

"REGISTERED PRINT" PRINTER	PRINTER DECRYPTS PACK WITH VENDORS PUBLIC KEY AND PRINTER'S PRIVATE KEY, AND EXTRACTS VENDORS SESSION KEY PRINTER DECRYPTS PRINT CONTENT WITH SESSION KEY AND CONTINUES PRINTING. 246
COMMUNICATIONS BETWEEN PRINTER AND BROWSER	
"USER BUY PRODUCT" CLIENT - BROWSER	244 BROWSER PLUG-IN/HELPER APP PASSES PACKET THROUGH TO PRINTER
NETWORK TRAFFIC BETWEEN CLIENT AND VENDOR	
VENDOR	
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND CLIENT	
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND VENDOR	
CREDIT HOLDER	
CA - CERTIFICATE AUTHORITY (E.G. GTE, VERISIGN)	

Fig. 2-12

"REGISTERED PRINT" PRINTER	
COMMUNICATIONS BETWEEN PRINTER AND BROWSER	PRINTER SENDS STATUS BACK TO BROWSER PLUGGIN/HELPER APP ON DECRYPTING SESSION KEY SUCCESS AND PRINT JOB SUCCESS. EACH PACKET IS ENCRYPTED WITH VENDORS PUBLIC KEY. "PRINT JOB SUCCESS" INCLUDES A "QUALITY/QUANTITY" COUNT FROM "GUARANTEED PRINT" ABILITIES. ~246
"USER BUY PRODUCT" CLIENT - BROWSER	EACH STATUS PACKET THE BROWSER RECEIVES FROM PRINTER STORED. EACH NEW PACKET OVERWRITES THE PREVIOUS.
NETWORK TRAFFIC BETWEEN CLIENT AND VENDOR	-- COMPLETE --
VENDOR	
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND CLIENT	
NETWORK TRAFFIC BETWEEN CREDIT HOLDER AND VENDOR	
CREDIT HOLDER	
CA - CERTIFICATE AUTHORITY (E.G. GTE, VERISIGN)	

Fig. 2-13

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

ATTORNEY DOCKET NO. 10001687-1

As a below named inventor, I hereby declare that:

My residence/post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Assured Printing Of Documents Of Value

the specification of which is attached hereto unless the following box is checked:

( ) was filed on _____ as US Application Serial No. or PCT International Application Number _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understood the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR 1.56.

Foreign Application(s) and/or Claim of Foreign Priority

I hereby claim foreign priority benefits under Title 35, United States Code Section 119 of any foreign application(s) for patent or inventor(s) certificate listed below and have also identified below any foreign application for patent or inventor(s) certificate having a filing date before that of the application on which priority is claimed:

COUNTRY	APPLICATION NUMBER	DATE FILED	PRIORITY CLAIMED UNDER 35 U.S.C. 119
			YES: ___ NO: ___
			YES: ___ NO: ___

Provisional Application

I hereby claim the benefit under Title 35, United States Code Section 119(e) of any United States provisional application(s) listed below:

APPLICATION SERIAL NUMBER	FILING DATE

U. S. Priority Claim

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION SERIAL NUMBER	FILING DATE	STATUS (patented/pending/abandoned)

POWER OF ATTORNEY:

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

Customer Number 022879

Place Customer Number Bar Code Label here

Send Correspondence to:
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80528-9599

Direct Telephone Calls To:
Raymond A Jenski
(541) 715-8441

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Inventor: Kevin G. Currans **Citizenship:** US

Residence: 883 Wyatt Lane Philomath OR 97370

Post Office Address: Same as residence

Kevin Currans
Inventor's Signature

8/15/2000
Date